

## NOAA Licensee Data Protection Template

### A. End-to-end process (high level)

1. Provide a high level description of the overall *data protection strategy*.
2. Provide a *flow diagram* that highlights the entire *data protection process*, from satellite tasking orders and decks to delivery of imagery and finished products.
3. Provide a *high level description* for the *end-to-end data protection process*. This description should delineate between protection methods implemented on the spacecraft (e.g., data encryption) and ground based protection methods (e.g., ground receiving station physical security). The combination of these protection methods must clearly implement the license conditions regulating commanding authority, tasking, imagery resolution and delivery time, country/regional access to imagery, etc.)

### B. Program Space Segment (detailed information)

Provide a brief description of the satellite system to include:

1. Orbital information (altitude, inclination, etc.)
2. Sensor type(s) (panchromatic, multispectral, hyperspectral, radar, etc.), basic design features [example: for EO systems, resolution (IFOV), imaging modes, spectral range (VNIR, SWIR, etc.), spectral bands (number of bands, center wavelength, bandwidth), swath width (FOV)] and scanning mechanism description(s) (pushbroom, step-stare, etc). Indicate which sensors produce co-registered imagery (e.g., by common optical systems) and which are independent (e.g., PAN and SAR).
3. Top-level platform properties (e.g., in-track and cross track pointing ability, on-board storage capacity, etc.)
4. General space/ground architecture (description with diagram).
5. Overview of the end-to-end system communications architecture (description with diagram)
6. RF data downlinks
  - a. Link information (top level description of the number of RF channels and the purpose of each)
  - b. Physical characterization of each link (frequency, modulation protocol, bit rates, link margin, beam patterns, data compression protocol, encryption methodology, etc.)
  - c. Information type(s) carried by each RF channel (e.g., tasking of image collection; telemetry, tracking, and control (TT&C), satellite health/status, imagery metadata, raw imagery data, etc.). The encryption level for each general information type must be specified.
7. Indicate whether the satellite incorporates separate tasking links and/or data protocols (e.g., encryption standards) for US Government and commercial operations. If separate processes exist, describe the differences in detail. This would include: encryption types used on all satellite up- and/or downlinks; key and re-key schemes;

and key management plans for each data, tasking, TT&C and/or relay links. Provide a separate key management plan for encryption protocols used directly with satellite operations and those used in ground relay and/or ground processing centers.

8. Provide a description of imagery data and metadata content and format, as well as any processes employed to alter image quality and/or information content (e.g., spatial/spectral pixel aggregation, discarding low-order A/D bits, data compression, etc.) in either the space or ground segment. This description should be “top level”, but should accurately represent any pre-processing, including compression of wideband image data, that takes place on board the spacecraft. It must include all on-board actions that result in changing data from their “raw or unenhanced” state to a “higher level” state (example: for EO systems, pixel aggregation/re-sampling affecting spatial or spectral resolution).

### **C. Program Ground Segment (detailed information)**

Provide a description of the ground segment to include:

1. Overview of system communications architecture (description with a diagram). This architecture includes all system-supporting ground stations (e.g., fixed, mobile, “bent pipe”, passive receipt with local processing, stations with command and/or data tasking authority, etc.)
2. Location of all satellite ground stations (including lat/long coordinates). Information on existing or planned mobile ground stations that are able to command, task, or receive data from the proposed system should be indicated. Owners and operators of foreign ground station facilities must be identified in detail, as well as any co-located data reception facilities at the ground station.
3. Personnel security (clearances, background checks, badging, access control), physical security (fences, gates, locks, guards, etc) within ground receiving stations and ground processing facilities. Treat each separately.
4. Protection (physical, electronic, storage, encryption, etc) afforded to processed or unprocessed imagery and associated metadata within ground receiving stations and ground processing facilities. Indicate level of protection afforded to TT&C and tasking lists within each facility possessing these authorities. Processing Center(s) imagery processing and distribution flow including:
  - a. Data relay methods and protection mechanisms between ground receiving stations and ground processing centers (by RF and/or physical transport). Highlight whether protection is accomplished by encryption or physical security (or both).
  - b. Protection mechanisms for end product during relay or delivery to licensed distributors, resellers, and value-added providers, as well direct sales to end-users. This requirement (examples might include physical security, separate delivery of encrypted files and the keys, etc.) is placed on both the licensee and their licensed distributors to inhibit diversion by proscribed entities.
5. USG agencies have a particular concern about revealing their requirements for commercial imagery data – including their lists of imagery tasking as a function of time and the actual imagery data sets that they have received. The licensee must provide a security plan that guarantees protection of this information and prevents its unauthorized release. The purpose of this requirement is not to remove imagery from the licensee’s archive; rather it is to remove the association of the datasets with the requirements of the USG.